In the Claims:

~~Please cancel claims 4-6, 9, 13-14, 16, and 20-21. Please amend claims 1 and 7. Please add new claims 22-30. The claims are as follows:~~

1. (Currently amended) A method enabling a network-addressable device to detect use of its identity by a ~~spoofer~~ spoofing vandal, comprising the acts of:

receiving a message by the network-addressable device from a target of a denial of service attack by the spoofing vandal, said attack comprising a denial of service communication sent by the spoofing vandal to the target;

detecting, by the network-addressable device, a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of [[a]] the denial of service attack on [[a]] the target by [[a]] the spoofing vandal using an identity of the network-addressable device in the denial of service communication, said detecting being performed after said receiving has been performed; and

generating, by the network-addressable device, a spoofing alert responsive to the act of detecting the communication protocol violation.

6

~~2.~~ (Original) A method enabling a network-addressable device to detect use of its identity by a spoofer, comprising the acts of:

receiving a message by the network-addressable device;

detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of activity of a spoofing vandal using the identity

of the network-addressable device in an attack on a target;

recording attributes of the message;

advancing the value of a counter associated with the target;

comparing the value of the counter with a predetermined threshold; and

generating a spoofing alert when the value of the counter exceeds the threshold.

7 6

~~3~~. (Previously presented) The method of claim ~~2~~, wherein the network-addressable device is connected to the target by a communication network.

4-6. (Canceled)

19 18

~~7~~. (Currently amended) The method of claim [[3]] ~~22~~, wherein said recording comprises recording said attributes of the message in a spoofing logbook database.

20 19

~~8~~. (Previously presented) The method of claim ~~7~~, wherein said recorded attributes of the message in the spoofing logbook database comprise a source address of the message, an indication of a nature of the activity of the spoofing vandal, and a time at which the message has been received.

9. (Canceled)

12 6

~~10~~. (Original) The method of claim ~~2~~, wherein the protocol violation includes reception by the network-addressable device of an unsolicited response message sent by the target.

13 6

~~11~~. (Original) The method of claim ~~2~~, wherein the protocol violation includes the reception by the network-addressable device of an ICMP reply sent by the target when an ICMP PING has not been sent to the target by the network-addressable device.

14 6

~~12~~. (Original) The method of claim ~~2~~, wherein the protocol violation includes reception by the network-addressable device of a SYN/ACK message when a SYN message has not been sent to the target by the network-addressable device.

13-14. (Canceled)

8 7

~~15~~. (Previously presented) The method of claim ~~3~~, further comprising providing a first network administrator who is responsible for the network-addressable device and a second network administrator who is responsible for the target.

16. (Canceled)

9 8

~~17~~. (Previously presented) The method of claim ~~15~~, wherein the first network administrator is a first automated network management system, and wherein the second network administrator is a second automated network management system.

10 7

~~18~~. (Previously presented) The method of claim ~~3~~, wherein the network-addressable device is connected to the spoofing vandal by the communication network.

11 7

~~19.~~ (Previously presented) The method of claim ~~5~~, wherein said detecting, recording, advancing, comparing, and generating are performed by the network-addressable device.

20-21. (Canceled)

18

~~22.~~ (New) A method enabling a network-addressable device to detect use of its identity by a spoofing vandal, comprising the acts of:

receiving a message by the network-addressable device from a target of a denial of service attack by the spoofing vandal, said attack comprising a denial of service communication sent by the spoofing vandal to the target;

detecting, by the network-addressable device, a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of the denial of service attack on the target by the spoofing vandal using the identity of the network-addressable device in the denial of service communication, said detecting being performed after said receiving has been performed;

recording attributes of the message;

advancing the value of a counter associated with the target;

comparing the value of the counter with a predetermined threshold;

generating a spoofing alert when a result of said comparing is that the value of the counter exceeds the threshold, said recording, advancing, comparing, and generating being performed by the network-addressable device.

21 18

~~23~~. (New) The method of claim ~~22~~, wherein the network-addressable device is connected to the target by a communication network, said method further comprising:

sending the spoofing alert to at least one network administrator selected from the group consisting of a first network administrator who is responsible for the network-addressable device, a second network administrator who is responsible for the target, and both the first network administrator and the second network administrator.

15 6

~~24~~. (New) The method of claim ~~2~~, wherein the protocol violation includes reception by the network-addressable device of an unsolicited response message sent by the target.

16 6

~~25~~. (New) The method of claim ~~2~~, wherein the protocol violation includes the reception by the network-addressable device of an ICMP reply sent by the target when an ICMP PING has not been sent to the target by the network-addressable device.

17 6

~~26~~. (New) The method of claim ~~2~~, wherein the protocol violation includes reception by the network-addressable device of a SYN/ACK message when a SYN message has not been sent to the target by the network-addressable device.

2

~~27~~. (New) The method of claim 1, wherein the network-addressable device is connected to the target by a communication network, said method further comprising:

sending the spoofing alert to at least one network administrator selected from the group consisting of a first network administrator who is responsible for the network-addressable device,

a second network administrator who is responsible for the target, and both the first network administrator and the second network administrator.

3

~~26.~~ (New) The method of claim 1, wherein the protocol violation includes reception by the network-addressable device of an unsolicited response message sent by the target.

4

~~29.~~ (New) The method of claim 1, wherein the protocol violation includes the reception by the network-addressable device of an ICMP reply sent by the target when an ICMP PING has not been sent to the target by the network-addressable device.

5

~~30.~~ (New) The method of claim 1, wherein the protocol violation includes reception by the network-addressable device of a SYN/ACK message when a SYN message has not been sent to the target by the network-addressable device.